# 臺中市畢業證書區塊鏈應用案例

臺中市政府資訊長 蕭景燈

臺中市西區大同國小教師 蕭聖哲



區塊鏈技術的第一個應用是數位貨幣，因此最初對此技術的探討多圍繞在金融財務相關領域，其不可竄改的基本特性讓區塊鏈不只是數位貨幣，也可以運用在任何價值的轉移交易、資料紀錄保存與跨機構共享，如再搭配智能合約，授權程式於滿足特定條件時不需人力介入自動執行，如此也增加了透明度與效能，對創業家而言區塊鏈意味著商業機會，但對提供公共服務的公部門而言，此項技術開啟了政府對人民服務的新模式。

對這個尚在探索階段的技術，各國政府投入的資源各異，努力的方向也不同，去（2017）年 9 月 Deloitte 發表了一份名為「區塊鏈將轉變公部門？」（Will blockchain transform the public sector?）[1] 的報告，報告中整理了包含

[1] https://www2.deloitte.com/insights/us/en/industry/public-sector/understanding-basics-of-blockchain-in-government.html

數位貨幣等 10 個公部門最積極推動的區塊鏈應用項目。此份報告在最終提出了建議，認為眾多方向中「身分管理」、「土地所有權登記」與「投票」是政府部門最能夠發揮區塊鏈價值的三項應用。

## 壹、結合內外部資源共同推動

臺中市政府在 2017 年起即思考區塊鏈運用於市民服務的可行性，經過內部討論，認為身分管理結合數位資產是適合在市府層級推動的應用，於同年 10 月與國家實驗研究院國家高速網路與計算中心簽訂合作備忘錄（圖 1），選定「畢業證書區塊鏈 PoC」為三個合作項目之一。畢業證書可以視為畢業生的無形資產，透過將此無形資產數位化，記錄在區塊鏈上，讓此項資產與畢業生的身分連結起來，將來對於此項資產的查詢或交易，任意第三方都不須透過原發證學校就可以進行畢業證書的驗證，這樣的過程沒有中介者，簡化了作業負擔，也提升了效益。

在市府內，這個 PoC 由資訊中心與教育局共同推動，並與教育局資訊教育暨網路中心相互配合，教網中心過去幾年負責 OpenID 單一帳號認證業務，亦是屬於身分管理的一環，兩個機制各司其職，透過介面設計達到互通，讓服務的整體性更佳。而教網中心原本就與學校行政人員與學生互動密切，因此可以負擔起在第一線服務使用者的角色。

## 貳、技術架構與流程設計

為了讓使用有個友善的操作介面，我們採用三層網路架構，包含後端底層的鏈，提供查詢的 Web Server，以及使用者端的瀏覽網頁呈現，圖 2 即是

國家高速網路與計算中心

臺中市政府與財團法人國家實驗研究院國家高速網路與計算中心

合作備忘錄

臺中市政府（以下簡稱甲方）與財團法人國家實驗研究院國家高速網路與計算中心（以下簡稱乙方）為臺中市政府市政服務應用區塊鏈技術進行合作事宜(以下稱本合作)，特簽訂本合作備忘錄(以下稱本備忘錄)，以作為確認雙方合作意願之依據，共同推動後續合作事項。

第一條　合作目的

甲乙雙方將協力推廣區塊鏈技術應用，並於「區塊鏈節點連結」、「單業證書區塊鏈　PoC」、「市府區塊鏈應用之協力發展」等主題開展具體合作事項。

第二條　合作範圍/合作模式

雙方為達成本備忘錄之合作目的，應就本合作具體合作之內容，訂立詳細之合作計畫；本合作具體合作內容之詳細分工、責任歸屬、費用、智慧財產權歸屬及其衍生之權益，應由雙方另行簽訂正式書面契約（以下簡稱正式契約），本備忘錄與正式契約有牴觸或不一致者，應以正式契約作為雙方之權利義務之依據。

第三條　保密義務

一、雙方應以善良管理人之注意，妥善保管因本備忘錄而知悉或持有之機密資訊，且非經他方事前書面之同意，不得洩漏或交付任何第三人。

二、機密資訊之所有權屬揭露之一方所有，除本備忘錄另有規定外，任一方依本備忘錄所為機密資訊之揭露，不應視為任何權利之授權。惟揭露方應於提供當時標示「機密」、「保密」或其他同義字，或其他方式使收受方可得而知其為商業上、技術上或生產上尚未公開之秘密，或雖未標示但需為一般商業及法律觀念，應視為機密之物品、文件及資料等。

三、本條保密義務，不因本備忘錄終止或解除而被免除。

第四條　權利歸屬

甲乙雙方依本備忘錄所產生成果之智慧財產權，依下列原則訂其歸屬：

一、由甲方或乙方人員獨力完成之成果，其智慧財產權分別歸甲方或乙方所有；

二、由甲方或乙方人員共同協力完成之成果，其智慧財產權依雙方貢獻比例歸甲方及乙方所有；

三、甲乙雙方得因個別工作計畫或專案之特殊情形，於進行合作前，另訂適用於各該個案之智慧財產權歸屬之其他約定。

國家高速網路與計算中心

臺中市政府與財團法人國家實驗研究院國家高速網路與計算中心

合作備忘錄

第五條　有效期間

本備忘錄自簽署日起生效，有效期為2年，得經雙方同意後提前終止，惟已在執行中[illegible]協議效力不受影響。如任一方欲終止本備忘錄應於1個月前以書面通知他方，本備忘錄[illegible]滿或有終止、解除事由，不影響第三條之效力。

第六條　一般條款

一、本備忘錄未盡事宜，由雙方本於誠信原則協商之。惟本備忘錄之增刪或修改，[illegible]事人以書面協議方式為之，不生效力。

二、本備忘錄係表彰甲乙雙方合作之意願，除第四條外，其餘條款對甲乙雙方不具法律[illegible]

三、凡因本備忘錄所生爭議，雙方同意本於誠信原則及商業習慣共同協議解決，若協[illegible]，應以中華民國法律為準據法，若因本備忘錄而涉訟者，雙方同意以臺灣臺中地[illegible]第一審管轄法院。

第七條　契約份數

本備忘錄壹式二份，由雙方各執乙份為憑。

立書人

甲　方：臺中市政府

代表人：林佳龍 市長

地　址：臺中市西屯區臺灣大道3段99號

乙　方：財團法人國家實驗研究院國家高速網路與[illegible]

代表人：謝繼堃 主任

地　址：臺中市中部科學工業園區科園路2號

中華民國一〇六年十月三日

**圖 1　臺中市政府與國家實驗研究院國家高速網路與計算中心合作備忘錄**

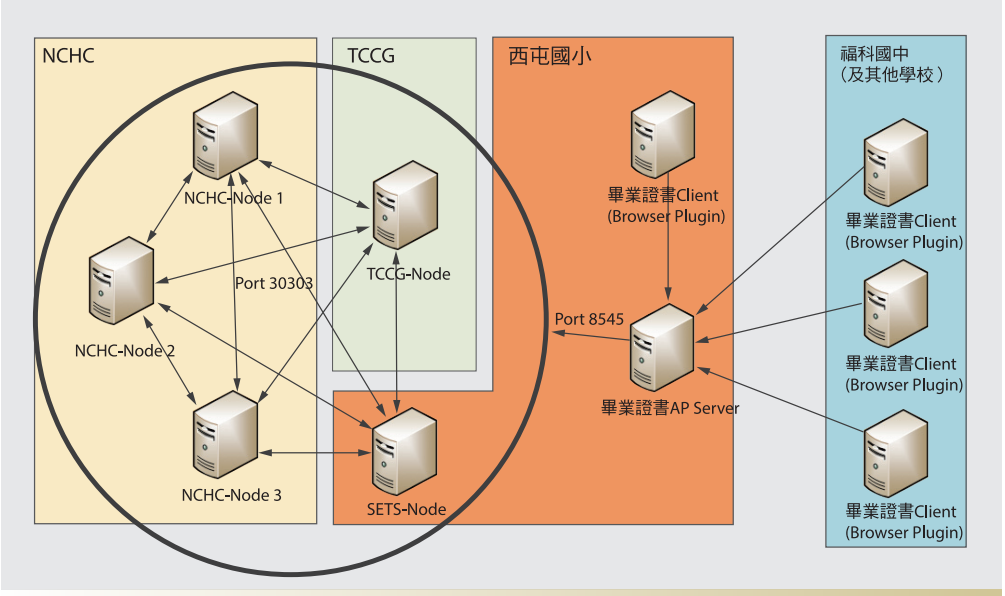


**圖 2　三層網路架構示意**

此三層網路架構之示意。

此外，我們選擇了乙太坊 Ethereum 做為區塊鏈底層平台，採用聯盟鏈架構，在圖 2 中顯示的聯盟鏈由五個節點組成，其中三個節點分別位於國網中心（NCHC）新竹、臺中、臺南三處機房，臺中市政府（TCCG）內另有一個節點，上述四個節點承擔運算工作，最後一個節點則置於臺中教網中心的西屯國小（STES）機房，這個節點也擁有鏈上完整的資料，但不負責運算而是與網站伺服器配合提供使用者查詢與瀏覽等服務。

本系統目前提供兩個主要機制，一是發行數位畢業證書至區塊鏈，二是自區塊鏈取出資料已驗證的數位畢業證書內容與簽署資訊；另有設計撤銷數位畢業證書機制會在日後版本新增。

數位畢業證書的發行由畢業生或是校方發起均可，最核心的步驟是校方對數位檔案中畢業證書記載內容進行審查，審查通過後，校方人員以審查人員的

私鑰則對此數位版本簽署，這相當於在實體複本蓋上「與正本相符」的戳記，並將此簽署過的文件加密儲存至分散式檔案系統 InterPlanetary File System（IPFS）並寫入區塊鏈。此簽署文件以 JSON Web Signature 格式提供給畢業生留存，我們也設計了較易攜帶與流通的 QR Code 圖片格式讓畢業證書所有人持有。

當畢業生繼續升學，進入下一階段的學校，新學校需驗證該名新生是否已由前一所學校畢業，過往普遍的方式就是要求新生繳交畢業證書，學校人員以肉眼查核；此系統提供了一個新的途徑，畢業生只需提交上述的 QR Code 圖片（當場出示或是透過電子郵件寄送），收到這個 QR Code 的一方可以用行動裝置掃描，連上驗證伺服器啟動本系統的驗證流程，當資料驗證無誤後，系統會回覆對應此 QR Code 的數位畢業證書下載點，此時驗證方由 IPFS 取回數位畢業證書就算是完成了 Proof of Existence，也就是相信有一筆畢業證書曾經發行並在此區塊鏈上昭告天下，上述發行寫入與驗證取出的兩個機制主

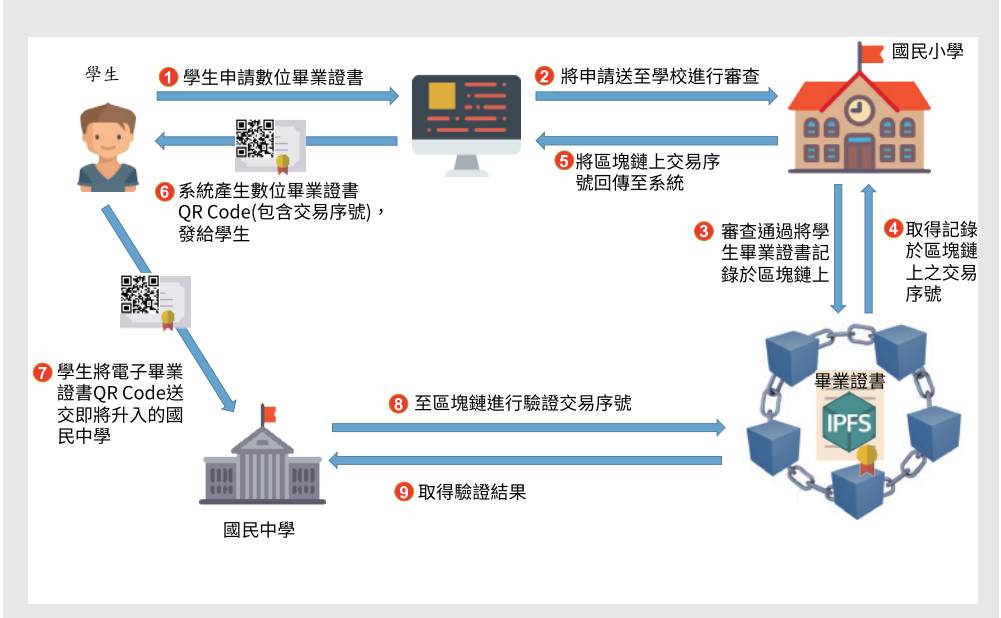


**圖 3　數位畢業證書發行寫入、驗證取出步驟**

要步驟如圖 3 所示。

未來可以進一步開發 App 讓學生管理自己的私鑰，驗證畢業證書的流程也可以加上向學生提出私鑰挑戰 Private Key Challenge，學生以透過此 App 回應挑戰，就可驗證該畢業證書所有權，更進一步做到 Proof of Ownership。

這樣的架構，把區塊鏈技術用到 Record Keeping 的實務上，一旦紀錄資料寫入區塊鏈，幾乎不可能被更動竄改，所以紀錄的安全性受到保障；而查詢資料的人可以用簡單快速的方式取得可信的資料，紀錄的可及性大幅提升，減少作業成本。

## 叁、實作成果

自去年底開始，國網中心開發團隊（圖 4）與市府同仁經過規格討論、節點架設、開發測試、介面調整等各種階段，在今年 6 月初提出了一個可以進入


**圖 4　國網中心開發團隊**

實際應用的版本，順利趕上小學的畢業季；在發展過程中教網中心阮志偉主任全力支持，而阮主任同時也是霧峰光正國小的校長，所以光正國小自然就成了此應用的示範學校。


**圖 5　光正國小張貼「介紹區塊鏈數位畢業證書」海報**

6 月 14 日光正國小畢業當日，老師在典禮會場貼上了介紹區塊鏈畢業證書的海報（圖 5），海報上有本屆 19 名畢業生的數位畢業證書驗證網址 QR Code，臺中市政府蕭景燈資訊長於現場掃描 QR Code，完成驗證，象徵性地頒發此畢業證書給畢業生（圖 6）。

## 肆、閱讀認證寫入區塊鏈，讓數位公民管理自己的數位資產

有鑑於臺中市政府與國家實驗研究院國家高速網路與計算中心合作之「畢業證書區塊鏈 PoC」於 6 月圓滿達成階段性任務，市政府資訊中心與教育局即刻思考如何將區塊鏈應用到更多教育場域。與學校關聯的應用即是由教育部資訊及科技教育司補助臺中市政府教育局進行的「臺中市線上閱讀認證系統」[2] 優化專案。

[2] http://read.tc.edu.tw/reading_certificate/


**圖 6　臺中市政府蕭景燈資訊長現場掃描 QR Code，完成驗證，象徵性頒發畢業證書**

閱讀認證系統主要目的在提供學生一個得以進行閱讀理解能力測驗的平台，學生必須先閱讀過實體書籍，再進入平台回答與該書相關的問題，並在正確率超過 80%以上，即取得該書的認證積分。隨著通過認證的書籍愈來愈多，學生也會取得相對應的閱讀鳥標章[3]，這些認證成績都可以視為學生學習過程累積的資產。不過，目前系統的登入帳號密碼必須藉由管理人員，以手動方式年年匯入，造成資料維護不易。同時，認證的資料是以資料庫方式儲存，若有遺失狀況發生，則學生的努力付之一炬。

閱讀認證系統的維護團隊（即是教育部委託臺中市政府教育局成立之「教育體系身分認證服務工作小組」）為了確保學生的閱讀認證資料可永久保

[3] http://read.tc.edu.tw/reading_certificate/back_home_2.php

存、永久有效且無法竄改，因此著手擴充「畢業證書區塊鏈 」的架構，藉區塊鏈技術來儲存學生的學習資料。同時為了也規劃建立一個臺中市政府教育局區塊鏈數位積點系統，將學習成就換算數位積點給予學生獎勵，在技術上即是一種 Asset Tokenization，這樣的區塊鏈不只是 Record Keeper 也是 Digital Currency。

閱讀認證系統將會是數位積點第一個運用的對象，學生在閱讀認證系統完成書籍認證並取得積分時，後端自動串接數位積點系統 API，將認證資料寫入區塊鏈之中，並產生一筆交易將獎勵的數位點數轉入學生的數位錢包。這些數位點數可以在錢包之間交換流通，累積的點數可以透由臺中市政府教育局的獎勵機制進行兌換，錢包內的點數兌換成實體獎品之後則直接銷毀。如此一來，這個點數機制間接促進學生的學習活動，達到更良好的學習成效。

現行有許多學習相關的網站也有虛擬點數設計，但是這些虛擬點數僅止於該網站內的運用，以舊的架構要實現跨站點數交換的成本太高並不可行。因此在閱讀系統優化專案運行順暢之後，工作小組預計規劃一個新的聯盟鏈，結合更多樣化的虛擬點數夥伴，讓區塊鏈分散共享的本質有最好的實踐。

## 伍、為數位原生代打造新世代的應用

臺中市區塊鏈的第一個試驗選擇教育學習場域，除了因為國民教育是地方政府的重要工作之外，也認知在學校階段的學生是熟悉各種數位工具的數位原生代（Digital Native）[4]，將區塊鏈應用引介至校園，引導學生了解這項科技，引發興趣與動機，藉以培養新世代數位國民。

[4] https://en.wikipedia.org/wiki/Digital_native